

Social Engineering: Hirngespinnst paranoider Sicherheitsexperten oder reale Gefahr?



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe & wie schütze ich mich davor?

Fazit, Fragen & Diskussion



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Motivation und Ziele dieses Vortrags

Ziel ist es, eine Sensibilisierung für die Thematik zu erzeugen

Nur für das Problem sensibilisierte Personen können SE-Angriffe erkennen und effizient abwehren

Die Herausforderung für jeden Einzelnen besteht darin, reine Freundlichkeit und Hilfsbedürftigkeit von Angriffsversuchen zu unterscheiden

Ziel ist **nicht** die eigene „Ausbildung“ zum Social Engineer! 😊





Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

„Social Engineering“ – Definitorisches

den Versuch, die menschliche Gesellschaft umzugestalten: *Social Engineering (Gesellschaftswissenschaft)*

eine (entwicklungs-)politische Tätigkeit, die aktiv soziale Gruppen schaffen und modulieren will: *Social Engineering (Politik)*

das gezielte Verwenden gestohlener Daten, um einer gutgläubigen Person weitere Daten wie z.B. Kennwörter oder Bankdaten zu entlocken: *Social Engineering (Sicherheit)*

[Quelle: Wikipedia, historisch]

Wie also lässt sich Social Engineering am Besten beschreiben?

Social Engineering ist DIE KUNST DER TÄUSCHUNG





Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

„Social Engineering“ – Abgrenzung und Einteilung

Die Erpressung oder die direkte Bedrohung von Personen zählt nicht zum Bereich des Social Engineering

Ein Social Engineer hat immer das Ziel, seine Aktivitäten unbemerkt durchzuführen

Es wird unterschieden zwischen

- Computer-Based Social Engineering
- Human-Based Social Engineering
- Reverse Social Engineering

Ein Social Engineer hat grundlegende Fähigkeiten eines Profilers

Profiler – eine Definition

Ein Profiler (Profilersteller, Fallanalytiker) erstellt Täterprofile. Die Tätigkeit bezeichnet man als operative Fallanalyse (profiling). Dabei erstellt der Profiler ein charakteristisches Erscheinungs- und Persönlichkeitsbild eines unbekanntes Straftäters anhand von Indizien, Spuren am Tatort und den Umständen der Straftat. Die Begriffe Profiler und Profiling leiten sich von (franz.) Profil= Umriss, Seitenansicht und von (italien.) profilo, profilare = umreißen ab.

[Quelle: Wikipedia, historisch]

Computer-Based Social Engineering

Beim „Computer-Based Social Engineering“ werden erforderliche Informationen mit technischen Hilfsmitteln beschafft.

Manipulierte Internetseiten, Mailanhänge oder Popup-Fenster mit Eingabefeldern sind nur einige Beispiele dafür.



Human-Based Social Engineering

Im Gegensatz zum Computer-Based Social Engineering werden beim „Human-Based Social Engineering“ die Informationen auf nicht-technischem Weg über die soziale Annäherung an Personen beschafft.

Eine weitere Ausprägung des Social Engineering ist das Reverse Social Engineering. Ziel des Angreifers ist es hier, sich die gewünschten Informationen über das Opfer nicht selbst zu beschaffen, sondern einen Anwender dazu zu bringen, die Informationen freiwillig und aktiv an den Angreifer zu übermitteln.

Beispiel: Der Angreifer stellt sich telefonisch als neuer Supportmitarbeiter beim Opfer vor und hinterlässt für auftretende Probleme seine Rufnummer. Danach sorgt er für ein Problem und erreicht damit, dass das Opfer ihn kontaktiert anstatt den zuständigen Unternehmenssupport um Hilfe zu bitten.

- **Vorteil:** Beim „Reverse Social Engineering“ ist die Chance wesentlich geringer, dass die Opfer Verdacht schöpfen.
- **Nachteil:** Aufgrund einer langen und intensiven Vorbereitung ist „Reverse Social Engineering“ allerdings ein sehr aufwendiges Verfahren. Oftmals muss ein Zugang zum Netzwerk oder Rechner des Anwenders bestehen, um diese Methode anwenden zu können.



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Wie sieht er aus – der typische Social Engineer?



Der Meister selbst: Kevin Mitnick



Ihr erster Kontakt mit einem Social Engineer

Wer war der erste Social Engineer, mit dem Sie Kontakt hatten?

IHRE EIGENEN ELTERN !!!



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Motivation und Ziele eines Social Engineers

Im Bereich der IT-Sicherheit ist ein Social Engineer im Prinzip ein „ganz normaler“ Krimineller

Meist handelt es sich um Auftragstäter, welche für ihren Auftraggeber sensible Informationen des Opfers stehlen sollen

Ethik ist für einen Social Engineer ein Fremdwort: er setzt bewusst Lug, Trug und Hinterlist ein, um an sein Ziel zu gelangen

Im Kundenauftrag operierende SE's interessieren sich nicht dafür, was mit den Informationen weiter passiert



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Welche Informationen sind für einen Angreifer nützlich?

Telefonlisten / Mitarbeiterlisten

Organigramme und Hierarchiestrukturen

Dienstleister und Zulieferer

Raumpläne

Dienst-, Schicht- und Urlaubspläne

Memos und Briefe

Netzpläne, Computernamen, Netzwerkadressen

Funktionsweise von Zugangskontrollsystemen

Prozessbeschreibungen (insbesondere aus dem Bereich des IT-Supports)

Arbeitsanweisungen und Policies

mangelnd sicher entsorgte Datenträger

Wie werden die Informationen beschafft?

Trashing / Dumpster Diving

Über das Telefon

Vor Ort

Informationsquelle Öffentlichkeit

- Internet / Suchmaschinen
- In der U-Bahn / im Zug
- Auf Festen (->“Bierlaune“)

Technische Hilfsmittel

- Keylogger
- Spyphones
- Kameras
- Mikrofone / Richtmikrofone

Verkleidung

(z.B. Uniform der Sicherheitsfirma, das Brustschild der Reinigungsfirma oder ein Blauemann mit Werkzeugkiste)

Die „Sprache“ des Opfers beherrschen

- Ansprache im Unternehmen („Du“ oder „Sie“)
- Abkürzungen (z.B. Abteilungsbezeichnungen)
- „*Firmenspezifisches Fachchinesisch*“

Die verschiedenen Typen von Angreifern (social)

- Angriff auf „Vertrauensbasis“
- Der „Hilfsbedürftige“
- Der „Moralische“ / Erzeugen von Schuldgefühlen
- Der „Insider“
- Der „Fachchinese“
- Der „Vorgesetzte“

Kombination mit technischen Angriffsformen (technical)

- Phishing
- Präparierte Internetseiten
- E-Mail – Anhänge
- Popup-Fenster
- „verlorene“ Wechselmedien (z.B. USB-Sticks)

news 12.06.2006 12:28



USB-Sticks als Trojanische Pferde der Neuzeit

In der griechischen Sage übertölpelte Odysseus die Einwohner Trojas noch mit einem vermeintlich zurückgelassenen, hölzernen Pferd. Seine Nachfolger arbeiten immer noch erfolgreich nach dem gleichen Prinzip: E-Mails mit angeblichen Nacktbildern – oder auch scheinbar verlorene USB-Sticks. Steve Stasiukonis von Secure Network Technologies **berichtet**[1] über einen interessanten Einbruchstest bei einer Kreditgenossenschaft, bei dem er über speziell präparierte USB-Sticks mehr interessante Daten in seinen Besitz bringen konnte, als er zu hoffen wagte.

Im Auftrag der Finanzexperten sollte Stasiukonis die Sicherheit des Netzes testen und dabei insbesondere auch in seine Social-Engineering-Trickkiste greifen. Anstatt mit den üblichen Schauspielertricks beim Smalltalk oder Flirt ein paar Informationen abzustauben, präparierten Stasiukonis und seine Mitarbeiter USB-Sticks unter anderem mit einem Keylogger, der Passwörter ausspionierte und dann per E-Mail verschickte. Von diesen modernen Trojanischen Pferden "verlor" Stasiukonis zwanzig auf dem Firmengelände. Die Angestellten konnten der Versuchung natürlich nicht widerstehen: Fünfzehn wurden gefunden und vom glücklichen Finder auch prompt in Firmenrechner gesteckt.

Ob für die anschließende Aktivierung des Keyloggers der Autorun-Mechanismus zum Einsatz kam oder die Angestellten aus Neugier die gefundenen Applikationen von Hand starteten, lässt sich dem Artikel zwar nicht entnehmen. Man darf aber wohl getrost annehmen, dass auch Letzteres passieren würde, wenn es der Angreifer geschickt genug anstellte.

Quelle: Trendmicro

14.07.2005

Neue Social Engineering-Techniken im Einsatz: Menschliche Tragödien sollen Neugierde wecken

Neuer Trojaner lockt mit Videoaufnahmen vom Terror-Anschlag in London

TREND MICRO (Nasdaq: TMIC, TSE:4704) hat mit TROJ_DONBOMB.A einen Trojaner identifiziert, welcher den aktuellen Bomben-Terror in London als Grundlage seiner Social Engineering-Technik verwendet. Der Trojaner verbreitet sich via eMail und enthält eine gefälschte Absenderadresse des Nachrichtensenders CNN. Im Textkörper wurde eine modifizierte HTML-Kopie der CNN-Webseite eingefügt, der Anhang verspricht Amateuraufnahmen des tragischen Vorfalls von vergangener Woche.

Der Trojaner TROJ_DONBOMB.A verwendet Social Engineering-Techniken, die in der jüngsten Vergangenheit auch bei anderer Malware immer häufiger zu beobachten sind: Um höhere Infektionsraten zu erreichen, täuschen die eMails vor, dass sie von einer bekannten und seriösen Nachrichtenagentur versendet wurden.

Die Verwendung eines konkreten und aktuellen Anlasses ist eine sehr bekannte und oft verwendete Methode bei Virenschreibern. Relativ neu ist aber das Vortäuschen der infizierten eMails, von einer bekannten Nachrichtenagentur abzustammen. Die Vermutung liegt nahe, dass diese Methode in Zukunft immer mehr an Bedeutung gewinnen wird.

Filmausschnitt aus „666“



Yps und der Münze...



Das Grundmotto der Social Engineers



Ein Beispiel aus der Praxis: Claudia Sorglos



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Die schlechte Nachricht zuerst:

Es gibt kein Patentrezept! 😞

**Es gibt keinen Patch für
menschliche Dummheit!**

Verhaltenstipps bei Anfragen einer nicht-verifizierten Person

Prüfung, ob die Person tatsächlich der- oder diejenige ist, für die sie sich ausgibt

- Rufidentifikation / Abgleich mit internem Telefonverzeichnis
- Rückruf
- Bürgschaft einer vertrauten Person
- Rückversicherung beim Vorgesetzten des Antragstellers
- eindeutige Identifikation anhand der Stimme
- In Person mittels eines Ausweises

Feststellung, ob der Antragsteller gegenwärtig bei der Firma angestellt ist oder die Beziehung solcherart ist, dass ein berechtigter Wissensbedarf besteht

- Nachschlagen im Mitarbeiterverzeichnis
- Verifikation über den Vorgesetzten oder einen Kollegen der Abteilung

Bestimmung, ob die Person dazu autorisiert ist, diese spezielle Information zu erhalten oder die gewünschte Handlung ausgeführt zu bekommen

- Einholen der Erlaubnis vom Vorgesetzten
- Freigabe durch den Eigentümer der Information

Verhaltenstipps bei Anfragen einer verifizierten Person

Feststellen, ob die Firma diese Person gegenwärtig beschäftigt oder eine Beziehung zu ihr hat die es ihr gestattet, Zugang zu den geforderten Informationen zu erlangen

Prüfen, ob diese Person zur Kenntnis der angefragten Information oder Handlung berechtigt ist

Passwörter

Passwörter sind im Grunde genommen wie Unterhosen:

- Wechselt sie oft
- Teilt sie nicht mit anderen
- Je länger desto besser
- Lasst sie nicht herumliegen

Der Post-It-Zettel mit dem Passwort am Arbeitsplatz ist immer noch unangefochten die Nummer 1 der Sicherheitslücken!

Generelle Tipps

Beim Verlassen des Raumes den Bildschirm des PCs sperren

Zugangsdaten zu Systemen nicht notieren oder schriftlich festhalten

Datenklassifizierung beachten oder, bei Nichtvorhandensein: eigene „Regeln“ aufstellen (öffentlich, intern, vertraulich/geheim) und Informationen demgemäß behandeln

Vertrauliche Unterlagen bei Abwesenheit grundsätzlich verschlossen aufbewahren

Vertrauliche Unterlagen generell sicher entsorgen (Papier in den Schredder, Datenträger durch spezielle Wipe-Programme löschen, etc.)

Beim Verlassen von Meetingräumen alle schriftlichen Aufzeichnungen (Flipchart, Whiteboard, etc.) entfernen und sicher verwahren

Mobiltelefone und PDAs wie den Arbeitsplatz-PC mit einem Passwort schützen



Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

- Es gibt kein „Schema F“ zur Erkennung
- Sei kritisch und hinterfrage die Dinge
- Betrachte nichts als selbstverständlich

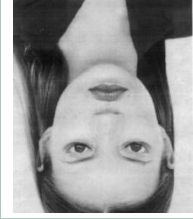
Literaturhinweise und Empfehlungen

- Kevin Mitnick *** Die Kunst der Täuschung (ISBN-13: 978-3826615696)
- Kevin Mitnick *** Die Kunst des Einbruchs (ISBN-13: 978-3826616228)
- Jens Eichler *** „Trau, schau, wem“ (<KES> 2007*1) (<http://www.eichler-online.net/TrauSchauWem.pdf>)
- Ein ehrenwerter Gentleman (DVD, Amazon-ASIN: B0000AGF7Z)
- 666 - Traue keinem, mit dem du schläfst (DVD, Amazon-ASIN: B00006L9R1)
- Takedown (DVD, Amazon-ASIN: B00008XQHK)

Vielen Dank!



Nochmal ... die **WICHTIGSTE** Regel



- Es gibt kein „Schema F“ zur Erkennung
- Sei kritisch und hinterfrage die Dinge
- Betrachte nichts als selbstverständlich

Nicht alles ist wirklich immer das, was es auf den ersten Blick zu sein scheint !!!

Jetzt aber endgültig: Vielen Dank!!

